DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy 6-2: Laptop Computers

1. References.

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. AR 380-67, Personnel Security Program, 9 September 1988.

   d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   e. DOD Instruction 8500.2, “Information Assurance (IA) Implementation”, 6 February 2003.

   f. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

   g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

   h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

   i. 4ID IA Policy 6-1 on Desktop Work Stations.

2. Purpose of Policy:

   a. This policy addresses methods and practices to manage Information Assurance (IA) risks inherent in laptop computers connected to, or storing information retrieved from, 4ID supported Automated Information Systems (AIS) and communications resources.

   b. Current 4ID AIS communications environments interleave trusted and public communications resources. This environment presents inherent IA risks to trusted military information resources regardless of whether connecting devices are fixed station desktop computers located on secured military facilities or whether they are portable devices using dial-in or wireless connectivity.

   c. Laptop computers provide additional IA risks (and challenges) that require means to safeguard stored information, when these devices are not located in trusted military facilities. Further, they require means to prevent unauthorized access to, or copying, of this information during dial-in or wireless connection to trusted systems and communications resources.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

a. Commanders, directors, and supervisors at all levels shall ensure that subordinate personnel are aware of their individual responsibilities to protect these valuable resources and use them in an authorized and effective manner.

b. The 4ID user community shall use automated resources responsibly and abide by normal standards of professional and personal conduct at all times.

c. All 4ID personnel shall report suspected laptop theft or unauthorized activity to their respective Information Assurance Manager (IAM), Information Assurance Network Manager/Officer (IANM/O), or Information Assurance Security Officer (IASO).

5. Policy - Laptop Computers:

a. Laptops are portable desktop workstations. As such, they are subject to the provisions of the 4ID Policy on Desktop Workstations unless specifically excepted in this policy.

b. Only laptop computers owned by the U.S. Army shall be provided connectivity to the 4ID automated information systems infrastructure. Unauthorized connection to the 4ID network will result in confiscation until the hard drive is wiped/purged by IA personnel.

c. Install IAVA patches and corrective patches as required:

d. Each laptop that requires remote connectivity to the 4ID network shall be connected via approved virtual private network (VPN) technology, when available.

e. The data stored on the hard drive of the laptop computer shall be encrypted using an approved method of encryption.

f. Access to the data stored on the laptop computer shall be restricted using an approved token assigned to the user to whom the laptop has been issued, or through sophisticated data encryption software requiring user ID and password access controls that are compliant with the 4ID password policy.

g. Wireless laptop connectivity to the 4ID network resources shall be allowed only upon approval of the 4ID IAM using DoD / NSA approved technology that facilitates a secure connection.

h. Laptops (notebooks) shall be configured to be C2 compliant or as close thereto as technically possible. The current Army security baseline configurations for laptop (notebook) operating systems are developed and maintained by Regional Computer Emergency Response Team – Europe (RCERT-C) and can be found at https://www.rcert-c.army.mil/.

i. Microsoft product baselines can be found at https://iassure.usareur.army.mil/security/microsoft/.

g. Changes to the configuration baseline of laptops shall be in accordance with the 4ID Configuration Management Plan (CMP) and coordinated and/or approved by the 4ID Configuration Control Board (CCB).

6. Non-compliance: Laptop workstations shall be reviewed on an ad hoc basis during maintenance in their useful life cycle. During routine maintenance, laptops shall be randomly inspected for compliance with the above policy.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding